Proposed CRL Processing Rules

Santosh Chokhani

chokhani@cygnacom.com

Briefing Contents

- Background
- Application Revocation Checking Requirements
- CRL Processing Rules

Background

- **Complete CRL for all entities**
  - Really complete (no issuing distribution point extension in CRL)
  - Complete with respect to asserted reason codes (only some reason codes field populated in the issuing distribution point extension of CRL)

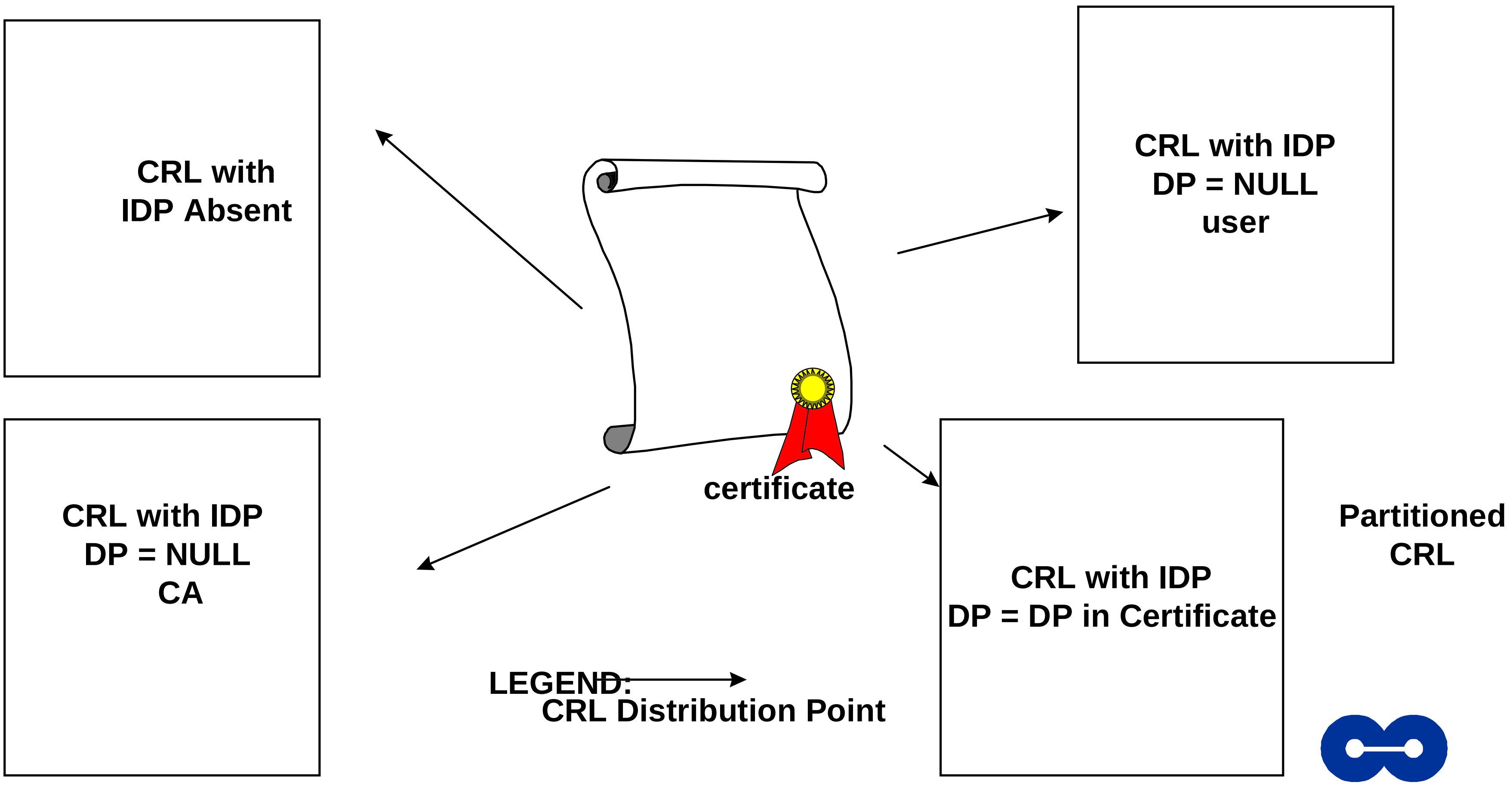
Background

- **Complete ARL**
  - Really complete (issuing distribution point extension in CRL has only onlyContainsCACerts field; field is set to TRUE)
  - Complete with respect to asserted reason codes (in addition to the above, only some reason codes field populated in the issuing distribution point extension of CRL)

Background

- **Complete CRL for end entities**
  - Really complete (issuing distribution point extension in CRL has only onlyContainsUserCerts field; field is set to TRUE)
  - Complete with respect to asserted reason codes (in addition to the above, only some reason codes field populated in the issuing distribution point extension of CRL)
  -

CRL Distribution Point



CRL with IDP Absent

CRL with IDP DP = NULL user

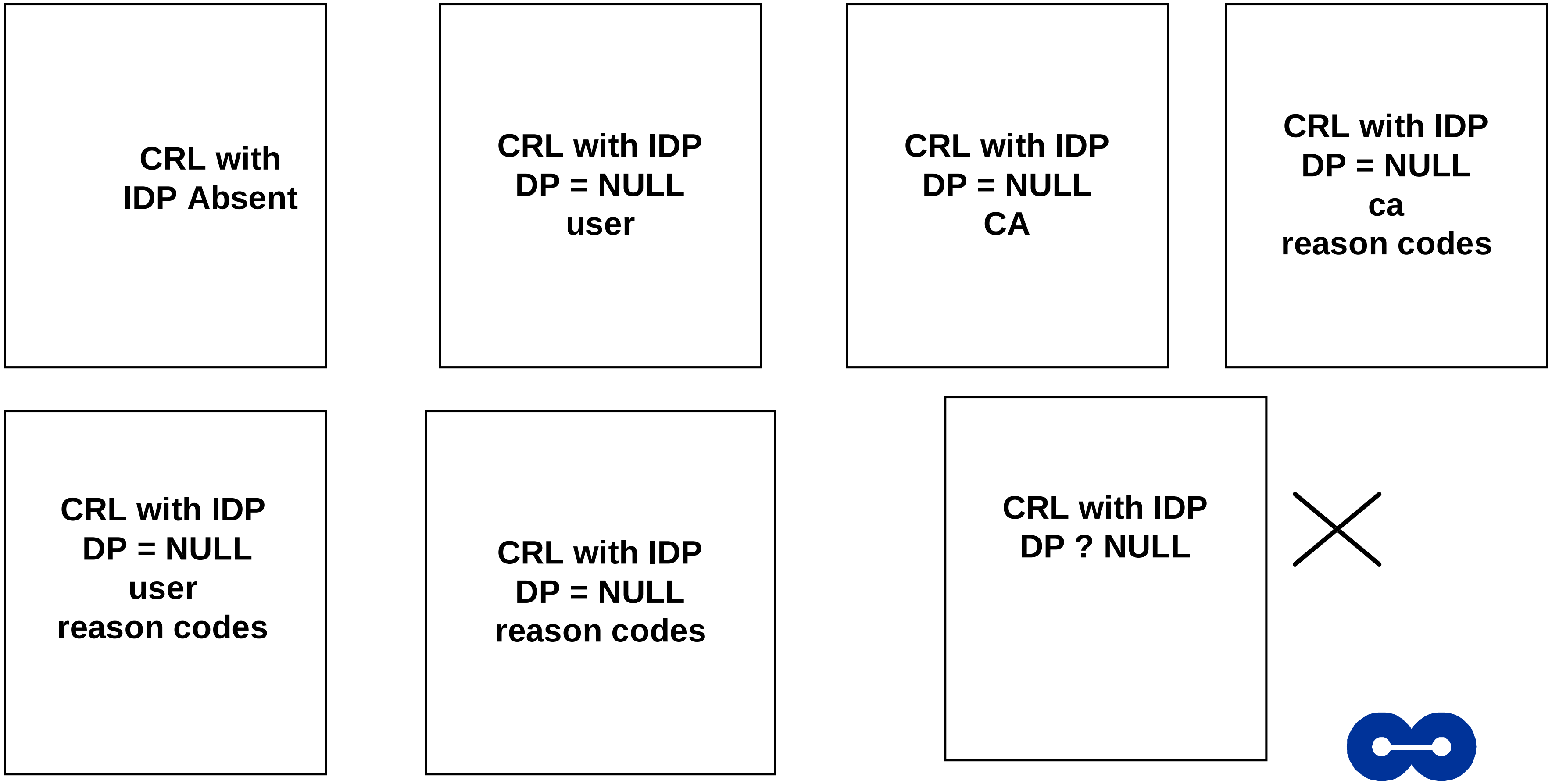
CRL with IDP DP = NULL CA

CRL with IDP DP = DP in Certificate

Partitioned CRL

LEGEND: → CRL Distribution Point

CRL In Issuer DN CRL & ARL Attribute



CRL with IDP Absent

CRL with IDP DP = NULL user

CRL with IDP DP = NULL CA

CRL with IDP DP = NULL ca reason codes

CRL with IDP DP = NULL user reason codes

CRL with IDP DP = NULL reason codes

CRL with IDP DP ? NULL

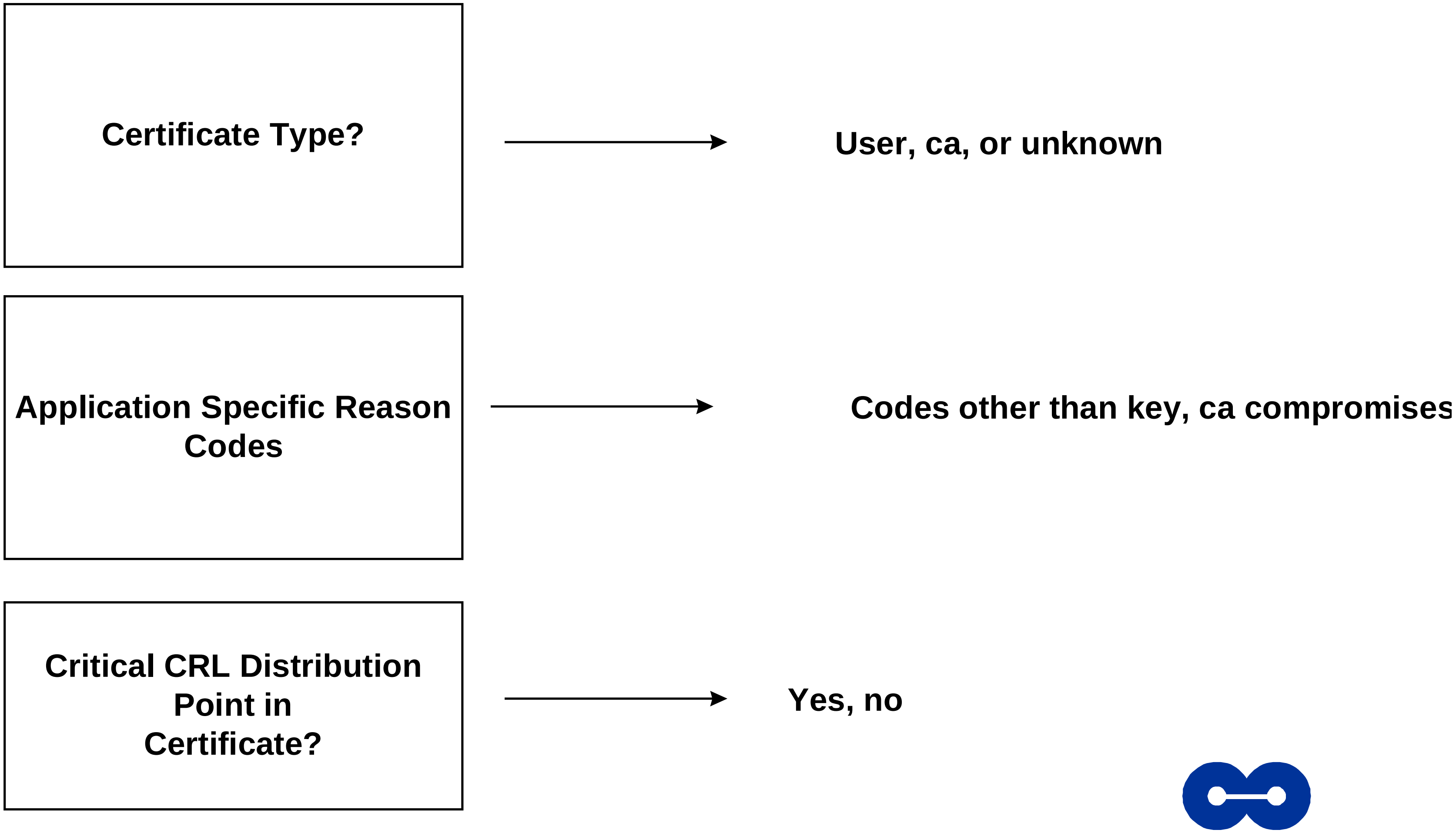
Certificate Types

End Entity Certificate (determined by presence of basic constraints extension)

CA Certificate (determined by presence of basic constraints extension)

Unknown Entity Type Certificate (determined by absence of basic constraints extension, otherwise rules could be numerous)

CRL Checking Flow Chart



Certificate Type? → User, ca, or unknown

Application Specific Reason Codes → Codes other than key, ca compromises

Critical CRL Distribution Point in Certificate? → Yes, no

Proposed Application Revocation Checking Requirements

- **End Entity Certificate**
  - key compromise reason code
  - other codes of interest determined by the application
- **CA Certificate**
  - ca compromise reason code
  - other codes of interest determined by the application
- **Unknown Entity Certificate**
  - key and ca compromise reason codes
  - other codes of interest determined by the application

End Entity Certificate: Critical CRL Distribution Point

- **Distribution point for key compromise reason code (distribution point field must appear in the CRL)**
- **Other reason codes of interest covered by the combination of the following**
  - Complete CRL for reason codes
  - Distribution points for reason codes
  - Complete end entity CRL for reason codes
- **Distribution point must point to CRL for all entities, CRL for End entities, or Partitioned CRL**

End Entity Certificate: No Critical CRL Distribution Point

- **Reason codes of interest = key compromise + Other reason codes of interest to application. Covered by a combination of the following**
  - – Complete CRL for reason codes
  - – Distribution points for reason codes
  - – Complete end entity CRL for reason codes
- **Distribution point must point to CRL for all entities, CRL for End entities, or Partitioned CRL**

CA Certificate: Critical CRL Distribution Point

- **Distribution point for ca compromise reason code (distribution point field must appear in the CRL)**
- **Other reason codes of interest covered by the combination of the following**
  - – Complete ARL for reason codes
  - – Complete CRL for reason codes
  - – Distribution points for reason codes
- **Distribution point must point to CRL for all entities, ARL, or Partitioned CRL**

CA Certificate: No Critical CRL Distribution Point

- **Reason codes of interest = ca compromise + Other reason codes of interest to application. Covered by a combination of the following**
  - Complete ARL for reason codes
  - Complete CRL for reason codes
  - Distribution points for reason codes
- **Distribution point must point to CRL for all entities, ARL, or Partitioned CRL**

Unknown Certificate: Critical CRL Distribution Point

- **Distribution point(s) for key and ca compromise reason codes (distribution point field must appear in the CRL)**
- **Other reason codes of interest covered by the combination of the following**
  - Complete CRL for reason codes
  - Distribution points for reason codes
- **Distribution point must point to CRL for all entities or Partitioned CRL**

Unknown Certificate: No Critical CRL Distribution Point

- **Reason codes of interest = key compromise + ca compromise + Other reason codes of interest to application. Covered by a combination of the following**
  - Complete CRL for reason codes
  - Distribution points for reason codes
- **Distribution point must point to CRL for all entities or Partitioned CRL**

Proposed CRL Processing Rules: Complete CRL

- Delta CRL indicator extension must be absent, and
- Issuing distribution extension may be present, and
- Issuing distribution point must not contain distribution point field, and
- Issuing distribution point extension must not contain onlyContainsUserCerts field, and
- Issuing distribution point extension must not contain onlyContainsCACerts field, and
- If the reasonCodes field is present in the issuing distribution point extension, the reasons code field must include all the reasons of interest to the application, and
- Issuing distribution point extension may contain indirectCRL field. No need to check for this field.

Proposed CRL Processing Rules: Complete ARL

- **Delta CRL indicator extension must be absent, and**
- **Issuing distribution extension must be present, and**
- **Issuing distribution point extension must not contain distribution point field, and**
- **Issuing distribution point extension must not contain onlyContainsUserCerts field, and**
- **Issuing distribution point extension must contain onlyContainsCACerts field. This field must be set to TRUE, and**
- **If the reasonCodes field is present in the issuing distribution point extension, the reasons code field must include all the reasons of interest to the application, and**
- **Issuing distribution point extension may contain indirectCRL field. No need to check for this field.**

Propsoed CRL Processing Rules: Complete End Entity

- Delta CRL indicator extension must be absent, and
- Issuing distribution extension must be present, and
- Issuing distribution point extension must not contain distribution point field, and
- Issuing distribution point extension must contain onlyContainsUserCerts field. This field must be set to TRUE, and
- Issuing distribution point extension must not contain onlyContainsCACerts field, and
- If the reasonCodes field is present in the issuing distribution point extension, the reasons code field must include all the reasons of interest to the application, and
- Issuing distribution point extension may contain indirectCRL field. No need to check for this field.

Proposed CRL Processing Rules: Partitioned CRL

- Either the distribution point field in the CRL’s issuing distribution point extension must be absent, or the distribution point field in the CRL distribution point extension of the certificate must match the distribution point field in the issuing distribution point extension of the CRL, and
- If onlyContainsUserCerts is set to TRUE in the issuing distribution point extension of the CRL, then the certificate being checked must contain basicConstraints extension with cA component set to FALSE and
- If onlyContainsCACerts is set to TRUE in the issuing distribution point extension of the CRL, then the certificate being checked must contain basicConstraints extension with cA component set to TRUE, and

Proposed CRL Processing Rules: Partitioned CRL (continued)

- Reasons code field in the issuing distribution point extension of the CRL must be absent if this field is absent in the CRL distribution point field of the certificate, and
- If the reasons code field is present in the CRL distribution point extension of the certificate, this field must be either absent from the issuing distribution point extension of the CRL or at least contain the reasons asserted in the CRL distribution point extension of the certificate, and
- If the cRLIssuer field is absent from the CRL distribution point extension of the certificate, the CRL must be signed by the CA, and

Proposed CRL Processing Rules: Partitioned CRL (concluded)

- If the cRLIssuer field is present in the CRL distribution point extension of the certificate, the CRL must be signed by the CRL Issuer identified in the CRL distribution point extension of the certificate and the CRL must contain the indirectCRL field in the issuing distribution point extension.